IN THE CLAIMS

Please cancel claims 19-27, amend claims 1, 10 and 16, and add new claims 28-31 as follows:

1. (CURRENTLY AMENDED) A method of operatively pairing a host receiver and a client receiver in a broadcast system, comprising:

(a) decrypting program materials generated by a service provider and received by the host receiver from the broadcast system;

(b) encrypting the decrypted program materials at the host receiver using a copy protection key;

(c) encrypting the copy protection key at the host receiver using a host-client pairing key generated by the service provider and shared between the host receiver and client receiver in order to share the program materials between the host receiver and client receiver, wherein the service provider establishes the host-client pairing key for a particular combination of the host and client receivers;

(d) transferring the encrypted program materials and the encrypted copy protection key from the host receiver to the client receiver;

(e) decrypting the transferred copy protection key at the client receiver using the host-client pairing key; and

(f) decrypting the transferred program materials at the client receiver using the decrypted copy protection key.

2. (ORIGINAL) The method of claim 1, wherein the program materials received by the host receiver are decrypted using a media encryption key.

3. (ORIGINAL) The method of claim 1, wherein the host-client pairing key is received by both the host receiver and the client receiver from the broadcast system.

4. (ORIGINAL) The method of claim 3, further comprising decrypting the host-client pairing key at the host receiver using a receiver key uniquely associated with the host receiver.

5. (ORIGINAL) The method of claim 4, wherein the copy protection key is generated by the host receiver using content information decrypted by the receiver key uniquely associated with the host receiver.

6. (ORIGINAL) The method of claim 5, wherein the content information comprises a content identifier.

7. (ORIGINAL) The method of claim 6, wherein the content identifier is obtained from the program materials .

8. (ORIGINAL) The method of claim 6, wherein the content identifier further comprises copy control information.

9. (ORIGINAL) The method of claim 3, further comprising decrypting the host-client pairing key at the client receiver using a receiver key uniquely associated with the client receiver.

10. (CURRENTLY AMENDED) An apparatus for operatively pairing a host receiver and a client receiver in a broadcast system, comprising:

(a) means for decrypting program materials generated by a service provider and received by the host receiver from the broadcast system;

(b) means for encrypting the decrypted program materials at the host receiver using a copy protection key;

(c) means for encrypting the copy protection key at the host receiver using a host-client pairing key generated by the service provider and shared between the host receiver and client receiver in order to share the program materials between the host receiver and client receiver, wherein the service provider establishes the host-client pairing key for a particular combination of the host and client receivers;

(d) means for transferring the encrypted program materials and the encrypted copy protection key from the host receiver to the client receiver;

(e) means for decrypting the transferred copy protection key at the client receiver using the host-client pairing key; and

(f) means for decrypting the transferred program materials at the client receiver using the decrypted copy protection key.

11. (ORIGINAL) The apparatus of claim 10, wherein the program materials received by the host receiver are decrypted using a media encryption key.

12. (ORIGINAL) The apparatus of claim 10, wherein the host-client pairing key is received by both the host receiver and the client receiver from the broadcast system.

13. (ORIGINAL) The apparatus of claim 12, further comprising means for decrypting the host-client pairing key at the host receiver using a receiver key uniquely associated with the host receiver.

14. (ORIGINAL) The apparatus of claim 13, wherein the copy protection key is generated by the host receiver using content information decrypted by the receiver key uniquely associated with the host receiver.

15. (ORIGINAL) The apparatus of claim 14, wherein the content information comprises a content identifier.

16. (CURRENTLY AMENDED) The apparatus of claim [[16]] 15, wherein the content identifier is obtained from the program materials .

17. (ORIGINAL) The apparatus of claim 16, wherein the content identifier further comprises copy control information.

18. (ORIGINAL) The apparatus of claim 12, further comprising means for decrypting the host-client pairing key at the client receiver using a receiver key uniquely associated with the client receiver.

19-27. (CANCELED)

28. (NEW) The method of claim 1, wherein the particular combination of the host and client receivers results in a different host-client pairing key for each pairing of the client receiver with the host receiver.

29. (NEW) The method of claim 1, wherein the particular combination of the host and client receivers results in the host receiver sharing the host-client pairing key with all client receivers.

30. (NEW) The apparatus of claim 10, wherein the particular combination of the host and client receivers results in a different host-client pairing key for each pairing of the client receiver with the host receiver.

31. (NEW) The apparatus of claim 10, wherein the particular combination of the host and client receivers results in the host receiver sharing the host-client pairing key with all client receivers.